Claims

1. An apparatus to enable operation of a computer by authorized users when in a secure mode of operation, the apparatus comprising:

a hub, the hub being configured to be in communication with the computer, the hub further including,

a card reader,

a hub microprocessor, and

an encryption engine;

a card, the card being configured for insertion into the card reader, the card including a card microprocessor; and

a user authentication device, the user authentication device being configured to validate the user as an authorized user of the card wherein, if the user is validated as the authorized user, the card microprocessor being configured to pass a key to the hub microprocessor in response to the validation of the user as the authorized user of the card, thereby activating the encryption engine of the hub to operate in the secure mode of operation.

2. The apparatus as recited in claim 1, wherein the hub includes a plurality of USB ports.

3. The apparatus as recited in claim 1, wherein the hub includes a plurality of FIREWIRE ports.

4. The apparatus as recited in claim 1, wherein the computer is connected to the hub through one of a USB or FIREWIRE interface.

5. The apparatus as recited in claim 1, wherein the user authentication device is a biometric scanner.

6. The apparatus as recited in claim 5, wherein the biometric scanner scans one of a fingerprint, an iris and a face.

7. The apparatus as recited in claim 1, wherein the card microprocessor includes a cryptographic microprocessor.

8. The apparatus as recited in claim 1, wherein the encryption engine includes a plurality of encryption/decryption channels.

9. The apparatus as recited in claim 1, wherein the hub includes control switches to bypass the hub to operate the computer in a non-secure mode of operation.

10. A computer security system for a computer, comprising:

an encryption control device, the encryption control device being in communication with the computer, the encryption control device including,

a card reader, the card reader being in communication with an encryption control device microprocessor,

a biometric identifier, and

an encryption engine;

a card, the card being adapted to be read by the card reader to validate a user as an authorized owner of the card in conjunction with the biometric identifier, wherein upon validation of the user, the encryption engine activates to create a secure environment.

11. The apparatus as recited in claim 10, wherein the encryption control device is portable.

12. The apparatus as recited in claim 10, wherein the encryption engine executes RSA public-key cryptosystem.

13. The apparatus as recited in claim 10, wherein the encryption control device is hot plugable.

14. The apparatus as recited in claim 10, wherein the encryption engine is a field programmable gate array.

15. The apparatus as recited in claim 10, wherein the card includes a card microprocessor, the card microprocessor being configured to execute a challenge/response protocol for establishing a secure path through the encryption control device.

16. An apparatus for providing a secure operating environment for a computer, the apparatus comprising:

an encryption control device, the encryption control device (ECD) being in communication with the computer, the ECD further including,

a card reader,

an ECD microprocessor,

an encryption engine, and

a biometric scanner;

a smart card, the smart card being configured for insertion into the card reader, the smart card including a smart card microprocessor, wherein upon the insertion of the smart card into the card reader, a secure path is established between the smart card microprocessor and the ECD microprocessor after completion of authentication of a user and completion of a challenge/response protocol, thereby unlocking an encryption engine to provide the secure operating environment.

17. The apparatus as recited in claim 16, wherein the ECD includes a storage medium for storing encrypted data.

18. The apparatus as recited in claim 16, wherein encrypted data is stored on a virtual drive of the computer.

19. The apparatus as recited in claim 16, wherein the continued presence of a user is monitored.

20. The apparatus as recited in claim 16, wherein the ECD is locked by a hot key sequence.